PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-341224
(43)Date of publication of application : 22.12.1998

(51)Int.Cl. H04L 9/32
E05B 49/00
G06F 12/00
G06F 15/00
H04Q 7/38
H04M 11/00
H04N 1/44
// G09C 1/00

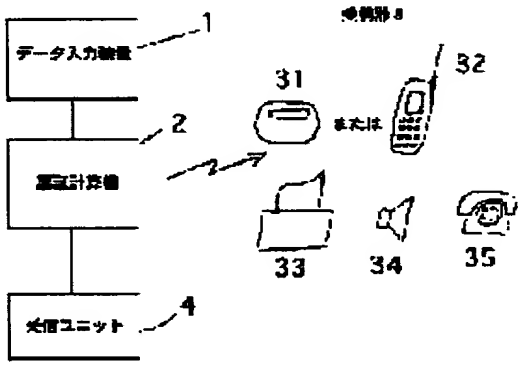
(21)Application number : 10-117449
(22)Date of filing : 27.04.1998

(71)Applicant : SCHMITZ KIM
(72)Inventor : SCHMITZ KIM

(30)Priority
Priority number : 97 19718103 Priority date : 29.04.1997 Priority country : DE

(54) AUTHENTICATION METHOD IN DATA TRANSMISSION SYSTEM AND SYSTEM TO EXECUTE THE AUTHENTICATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To transmit data with high security by allowing an authentication computer to use a random number generator so as to generate an alphanumeric transaction number TAN or a password, sending it to a receiver via other transmission path in parallel with a line connecting the authentication computer to a data entry device and authenticating the number or the password and connecting to the user.
SOLUTION: An authentication computer 2 generates a TAN or a password by a TAM or password generation or return request via a data entry device 1, and transmits it to a receiver 3 such as a pager 31 or a portable telephone set 32. Then the user receives it from the receiver and reads or hears it from a speaker 34, enters the TAN or password to the data entry device 1, which sends the TAN or the password to the authentication computer 2, which checks the validity. When the TAN or the password is valid, the authentication computer 2 forms connection to the reception unit 4. The user can transmit and/or receive data from the data entry device 1 to the equipment unit 4 while the connection continues. Furthermore, the connection time is limited to avoid the data entry device 1 and the reception unit 4 from being continuously connected.



LEGAL STATUS
[Date of request for examination]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－341224

(43)公開日　平成10年(1998)12月22日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７３Ｄ
Ｅ０５Ｂ	49/00		Ｅ０５Ｂ	49/00	Ｊ
					Ｒ
Ｇ０６Ｆ	12/00	５３５	Ｇ０６Ｆ	12/00	５３５Ｄ
	15/00	３３０		15/00	３３０Ａ

審査請求　未請求　請求項の数23　ＯＬ　（全 6 頁）　最終頁に続く

(21)出願番号　特願平10－117449

(22)出願日　平成10年(1998)４月27日

(31)優先権主張番号　１９７１８１０３．１

(32)優先日　1997年４月29日

(33)優先権主張国　ドイツ（ＤＥ）

(71)出願人　598055943
キム　シュミッツ
ドイツ連邦共和国　ミュンヘン　フンボルトシュトラーセ　19

(72)発明者　キム　シュミッツ
ドイツ連邦共和国　ミュンヘン　フンボルトシュトラーセ　19

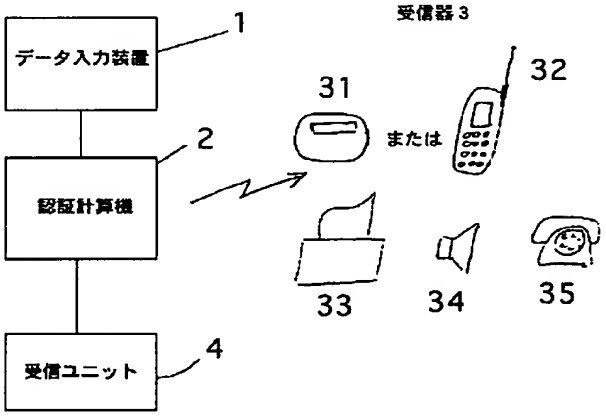
(74)代理人　弁理士　矢野　敏雄　（外３名）

(54)【発明の名称】　データ伝送システムにおける認証方法および認証方法を実施するための装置

(57)【要約】

【課題】　トランザクション番号（ＴＡＮ）を使用するデータ伝送システムにおいて、安全な認証方法および装置を提供すること。

【解決手段】　本発明による方法では、第1ステップで、利用者がデータ入力装置を介して自分の識別子および／またはデータ入力装置の識別情報と、ＴＡＮの生成要求またはデータからの選択要求とを、認証計算機に送信し、第2ステップで、認証計算機はＴＡＮを生成またはファイルから選択し、第3ステップで、認証計算機はＴＡＮを、第1ステップとは別の伝送経路を介して受信器に送信し、第4ステップで、利用者は前記ＴＡＮを前記受信器から受け取り、前記データ入力装置に入力し、第5ステップで、前記ＴＡＮを再び前記認証計算機に伝送し、第6ステップで、認証計算機は前記ＴＡＮの有効性を検査し、第7ステップで、前記データ入力装置と受信ユニットとの接続を確立または解放する。



1

【特許請求の範囲】

【請求項1】　トランザクション番号（ＴＡＮ）または同等のパスワードを使用するデータ伝送システムにおける認証方法において、

第1ステップで、利用者がデータ入力装置（１）を介して自分の識別子および／またはデータ入力装置（１）の識別情報を、ＴＡＮまたは同等のパスワードの生成要求またはファイルからの選択要求とともに、認証計算機（２）に送信し、

第2ステップで、前記認証計算機（２）は前記ＴＡＮまたは同等のパスワードを生成し、またはファイルから選択し、

第3ステップで、前記認証計算機（２）は前記ＴＡＮまたは同等のパスワードを、第1ステップとは別の伝送経路を介して受信器（３）に送信し、

第4ステップで、利用者は前記ＴＡＮまたは同等のパスワードを前記受信器（３）から受け取り、前記データ入力装置（１）に入力し、

第5ステップで、前記ＴＡＮまたは同等のパスワードを再び前記認証計算機（２）に伝送し、

第6ステップで、前記認証計算機（２）は前記ＴＡＮまたは同等のパスワードの有効性を検査し、

第7ステップで、前記データ入力装置（１）と受信ユニット（４）との接続を確立または解放することを特徴とする方法。

【請求項2】　前記ＴＡＮまたは同等のパスワードは、1回だけ使用することのできる請求項1に記載の方法。

【請求項3】　前記ＴＡＮまたは同等のパスワードの有効性は、所定の利用者時間によって決まる請求項1または2に記載の方法。

【請求項4】　前記ＴＡＮまたは同等のパスワードの有効性は、伝送されるファイルの所定の数に依存する請求項1から3までのいずれか1項に記載の方法。

【請求項5】　前記ＴＡＮまたは同等のパスワードの有効性は、伝送されるファイルの所定のサイズに依存する請求項1から4までのいずれか1項に記載の方法。

【請求項6】　前記データ入力装置（１）および／または前記受信器（３）および／または前記受信ユニット（４）に対するアクセスは、パスワードで保護されている請求項1から5までのいずれか1項に記載の方法。

【請求項7】　前記データ入力装置（１）から前記受信ユニット（４）に、または逆方向に伝送されるデータは、暗号化されている請求項1から6までのいずれか1項に記載の方法。

【請求項8】　前記データ入力装置（１）から前記認証計算機（２）に、または逆方向に伝送されるデータは、暗号化されている請求項1から7までのいずれか1項に記載の方法。

【請求項9】　前記受信器（３）はページャ（３１）であることを特徴とする請求項1から8までのいずれか1項に記載の方法を実施するための装置。

2

【請求項10】　前記受信器（３）は携帯電話（３２）である請求項1から8までのいずれか1項に記載の方法を実施するための装置。

【請求項11】　前記受信器（３）はテレファックス（３３）である請求項1から8までのいずれか1項に記載の方法を実施するための装置。

【請求項12】　前記受信器（３）は電子メールアドレスまたは網アドレスである請求項1から8までのいずれか1項に記載の方法を実施するための装置。

【請求項13】　前記受信器（３）は音声出力装置である請求項1から8までのいずれか1項に記載の方法を実施するための装置。

【請求項14】　前記音声出力装置はスピーカ（３４）である請求項11に記載の装置。

【請求項15】　前記音声出力装置は電話（３５）である請求項11に記載の装置。

【請求項16】　前記受信器（３）は、データ入力装置（１）に組み込まれた無線受信器であり、

該無線受信器は前記ＴＡＮまたは同等のパスワードを前記データ入力装置（１）のディスプレイまたはモニタに出力することを特徴とする請求項1から13までのいずれか1項に記載の方法を実施するための装置。

【請求項17】　前記無線受信器は、利用者識別部材を有する請求項14に記載の装置。

【請求項18】　前記利用者識別部材は、磁気カードまたはＩＣカードである請求項15に記載の装置。

【請求項19】　前記利用者識別部材は、指紋検査または利用者の画像識別のためのグラフィック装置と動作する請求項15に記載の装置。

【請求項20】　前記認証計算機（２）と前記受信器（３）に同じ暗号化モジュールを有する請求項1から17までのいずれか1項に記載の方法を実施するための装置。

【請求項21】　前記受信ユニット（４）はドア閉鎖機構である請求項1から18までのいずれか1項に記載の方法を実施するための装置。

【請求項22】　前記認証計算機（２）と前記受信ユニット（４）が1つの装置に統合されている請求項1から19までのいずれか1項に記載の方法を実施するための装置。

【請求項23】　前記データ入力装置と、前記認証計算機（２）および前記受信ユニット（４）が1つの装置に統合されている請求項1から19までのいずれか1項に記載の方法を実施するための装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はデータ伝送システムにおける認証方法およびこの方法を実施するための装置に関する。

3

【０００２】

【従来の技術】テレバンキングの際に、利用者はトランザクション毎に恒久的なパスワード（ＰＩＮ）の他に付加的にトランザクション番号（ＴＡＮ）が必要であることは公知である。このようなＴＡＮは多くの地域で利用者に郵便で送達される。したがって、このＴＡＮの第三者が情報を入手することができたり、パスワードに関して悪用が行われうる危険性がある。この危険性は、このＴＡＮが事実上無制限な有効期間があることによって、さらに高まっている。

【０００３】またコールバックシステムも公知である。コールバックシステムでは、呼び出された側のシステムが、通常は記憶された番号でコールバックすることによって、呼び出し側のシステムが権限を有し、権限のないシステムが権限のあるシステムと偽っていないかを確認する。コールバックシステムの欠点は、権限のない利用者が認証された呼び出し側システムへの機能的なアクセス権を任意のソースからから入手することができると、違法に得たこの認証のもとで問題なく作業できることである。というのはコールバックシステムは、基本的に認証されたシステムから呼び出されたか否かを検査するだけだからである。

【０００４】

【発明が解決しようとする課題】本発明は、安全性の高い、データ伝送における認証の方法を提供することを課題とする。

【０００５】

【課題を解決するための手段】上記課題は本発明の請求項1の特徴により、トランザクション番号（ＴＡＮ）または同等のパスワードを使用するデータ伝送システムにおける認証方法において、第1ステップで、利用者がデータ入力装置を介して自分の識別子および／またはデータ入力装置の識別情報と、ＴＡＮまたは同等のパスワードの生成要求またはファイルからの選択要求とを、認証計算機に送信し、第2ステップで、認証計算機はＴＡＮまたは同等のパスワードを生成またはファイルから選択し、第3ステップで、認証計算機はＴＡＮまたは同等のパスワードを、第1ステップとは別の伝送経路を介して受信器に送信し、第4ステップで、利用者は前記ＴＡＮまたは同等のパスワードを前記受信器から受け取り、前記データ入力装置に入力し、第5ステップで、前記ＴＡＮまたは同等のパスワードを再び前記認証計算機に伝送し、第6ステップで、認証計算機は前記ＴＡＮまたは同等のパスワードの有効性を検査し、第7ステップで、前記データ入力装置と受信ユニットとの接続を確立または解放することを特徴とする方法およびこの方法を実施するための装置を構成することによって解決される。

【０００６】

【発明の実施の形態】例えば携帯電話やページャのような無線の遠距離通信装置は、短い（英）数字情報（例えばＳＭＳサービス、Short Message Service）を受信し、そのディスプレイに表示する機能を有していることも多い。本発明はこの機能を利用して、ＴＡＮまたは同等のパスワードを伝送する。

4

【０００７】本発明では、利用者はデータ入力装置を介して自分の識別情報（ユーザＩＤ、パスワード等）および／またはデータ入力装置の識別情報を　、ＴＡＮ（または同等のパスワード）の生成要求とともに、認証処理を行う計算機に伝送する。以下ではこの計算機を略して認証計算機と呼ぶ。この認証計算機は、乱数発生器によって英数字または数字のみからなるＴＡＮ（または同等のパスワード）を計算したり、ファイルから取り出す。つぎにこの認証計算機からデータ入力装置との間に設けられている接続と並列に、別の伝送経路を介してこのＴＡＮ（または同等のパスワード）が受信器に伝送される。このような受信器の例としては、

ａ）　携帯電話、ページャ（例えばポケベル）のようなディスプレイまたはモニタを有する無線受信器。

【０００８】ｂ）　専用に形成されたデータ入力装置内の受信カード。この受信カードは無線または固定の配線を介して呼び出される。

【０００９】ｃ）　受信箱

ｄ）　テレファクス

ｅ）　音声出力装置。例えば固定的に設置されたスピーカ、または電話。

【００１０】さらに認証計算機は、必要となる電話番号、無線番号、ファックス番号、電子メールアドレスまたは網アドレスを使用できる。このような関連するデータは通常は認証計算機に記憶されている。しかし認証計算機そのものがこのようなデータを、別の計算機にあるデータバンクから取り出すことも可能である。この点では本発明による方法を使用する認証計算機そのものが、別の計算機へのアクセスを行うこともあり得る。

【００１１】認証された利用者は、上記のように伝送されたＴＡＮ（または同等のパスワード）を手動でデータ入力装置に入力し、再び認証計算機に送信することができる。本発明では自動化された方法の場合に、ＴＡＮ（または同等のパスワード）の自動的な送信が行われる。ここで認証計算機は、すべての（認証計算機から与えられた）有効なＴＡＮ（または同等のパスワード）との一致を検査し、この認証検査後にデータ入力装置と受信ユニットとの間のデータ流を許可する。

【００１２】本発明の場合のＴＡＮ（または同等のパスワード）は、１回だけ使用できるＴＡＮである。しかしながら利用者時間および／またはＴＡＮ（または同等のパスワード）の伝送データの数またはサイズのような、他の制限をＴＡＮの有効性に対して考慮することも可能である。

【００１３】上に記載した方法で認証され、接続が確立された後には、データ入力装置からのデータは受信ユニ

5

ットに（またはその逆方向；または全二重で）伝送することができる。

【００１４】付加的なセキュリティのためにこのデータを暗号化することも可能であることは明らかである。

【００１５】データ入力装置だけでなく、認証計算機と受信ユニットは通常の（パーソナル）コンピュータでよい。本発明は、プラットホームに無関係に有効である。すなわち本発明は、プロセッサのタイプ、オペレーティングシステムおよび／または制御電子機器（例えば受信ユニット）および／または（例えばデータ入力装置と受信ユニットの）入出力ユニットに依存しない。

【００１６】本発明によるシステムのセキュリティの本質的な点は、装置を認証した場合にのみ、認証計算機がデータ入力装置から受信ユニットへのデータ伝送を可能とすることである。これは、一つはデータ入力装置と認証計算機との間の伝送路、もう一つは認証計算機とＴＡＮ伝送装置との間の伝送路と、別々の伝送路を設けたことによって達成される。この点で本発明とコールバックシステムとは異なる。コールバックシステムでは、データ入力装置と認証計算機との間でただ一度だけ検査が行われる。

【００１７】本発明による方法では、種々異なるセキュリティレベルが可能である。

【００１８】本発明によるもっとも低いセキュリティレベルでは、データ入力装置に、受信器として無線受信器、例えばスロットカードの形態の無線受信器を組み込み、この専用の装置を使用した場合にのみ受信ユニットへのデータ伝送が可能となるようにする。このセキュリティを高めるために、無線受信器が利用者識別部材、例えば磁気カードまたはＩＣカードを使用した場合のみ動作するようにしてもよい。この利用者識別部材は、また利用者の指紋の検査や画像識別のような図形による手段で動作するようにしてもよい。

【００１９】本発明による別のセキュリティレベルでは、認証計算機がＴＡＮ（または同等のパスワード）をページャまたは類似の装置に伝送する。この場合に、データ入力装置とページャが同一人物によってアクセス中である場合にのみ、認証が行われる。そしてこの場合にのみ、ページャのディスプレイに表示されたＴＡＮ（または同等のパスワード）をデータ入力装置に入力し、さらにそこからデータを認証計算機に再び伝送することができる。

【００２０】しかしページャに伝送されたデータは公知の方法によって盗聴される可能性もある。本発明による別のセキュリティレベルでは、認証計算機とページャに同じ暗号化モジュールを設けることによって達成される。

【００２１】本発明による方法ではページャーまたは携帯電話の代わりに、別の受信装置を設けることもできる。このような装置としては、受信箱、テレファックス

6

または音声出力装置がありうる。本発明では音声出力装置としては、固定的に設置されたスピーカ、または所定の電話接続上への音声の伝送であってもよい。音声出力装置では、ＴＡＮ（または同等のパスワード）の音声出力が行われる。

【００２２】このような受信装置への伝送も暗号化してもよいことも明らかである。

【００２３】ページャの代わりに携帯電話、例えばＧＳＭ携帯電話が用いられた場合は、ＧＳＭ携帯電話に関する伝送技術の暗号化があるため、本発明で別の暗号化機構を用いなくてもよい。この場合にＴＡＮ（または同等のパスワード）は携帯電話のディスプレイに表示される。

【００２４】本発明による別のセキュリティレベルでは、データ入力装置と認証計算機との間は、このデータ入力装置を介して相応するパスワードが伝送された場合にのみ接続される。このパスワードは本発明では実質的にＴＡＮよりも時間的に長い有効期間を有する。

【００２５】本発明による別のセキュリティレベルでは、データ入力装置を利用するためにまずパスワードが同じように必要とされる。

【００２６】上の記載したセキュリティレベルを組み合わせることができることは明らかである。

【００２７】本発明は、データ伝送システムの分野において一般的に投入することができる。例えばインターネット、イントラネット、ローカルエリアネットワーク（ＬＡＮ）、ワイドエリアネットワーク（ＷＡＮ）その他に対しても有効である。

【００２８】本発明によるシステムでは、従来からのＥＤＰ分野以外でも、例えば物理的な入室制御の場合にも利用可能である。この場合に利用者は、例えばドアのそばに設けられたキーボード（＝データ入力装置）に自分のパスワードを入力する。認証計算機はこのパスワードを、場合によっては特定の部屋への特定の時間帯での入室権限に関しても検査する。当該パスワードが（いまなお）有効であれば、認証計算機は携帯電話、またはドア閉鎖システム専用に考案された、機能的にはページャと同等の装置に、ＴＡＮ（または同等のパスワード）を伝送する。引き続いてこのＴＡＮ（または同等のパスワード）は、利用者によってドアの近くに設けられたキーボードを介して手動で入力され、自動的に認証計算機に伝送される。検査に合格すると認証計算機からドア閉鎖機構を開放する信号が出力される。開放は場合によっては時間的に制限してもよい。この場合に受信ユニットは技術的な観点からは簡単な性質のものでよい。というのは受信ユニットはドア閉鎖機構を開放する信号を加工して、電気的機構を開放しドアに開くようにするだけだからである。

【００２９】上に記載したことから、個々人に応じてそれぞれ異なる部屋への入室のために、それぞれ異なる認

証を有するシステムを構成することが可能となる。

【００３０】具体的な応用分野にはつぎのようなものがある。例えば、

－　計算機センタ
－　空港
－　省庁
－　税関
－　国境通過
－　保安警部部門
－　銀行
－　金庫
－　ガレージ
－　駐車場
－　自動車

総合的なシステムは専用のセキュリティを有しており、このセキュリティには複数の、種々異なるつぎのような基本原理と要因の組み合わせられている。

【００３１】（１）　利用者だけが有している物(what-you-have)（複製できない（ＧＳＭ）チップ）、すなわち物理的に唯一な物。紛失して他人の手に渡ることもある。

【００３２】（２）　利用者だけが知っていること(what-you-now)（ＧＳＭ　ＩＣカードのＰＩＮと、データ入力装置および／または認証サーバの専用の利用者名）、すなわち知識。これは意図なくして、または不注意では他人の手に渡ることはない。

【００３３】（３）　ＤＥＳ暗号化およびＧＳＭ網そのものの暗号認証、盗聴および改竄に対する防御。

【００３４】このために1つ1つでは非常に希な、少なくともつぎの3つの事象がなければ、システムへの信頼性が失われることはない。

【００３５】a）　（携帯）ＩＣカード、ページャーの紛失。または受信箱、テレファックスまたは音声出力装置への他人のアクセス。

【００３６】b）　受信者のＰＩＮの漏洩（例えばＩＣカードまたは携帯電話から）

c）　伝送されたＴＡＮまたは同等のパスワードの情報誤りからこのような要因が同時に発生することは可能な限り回避しなければならない。しかしこのような場合でもシステムへの侵入が成功するためにはアクセス方法についての詳しい知識と利用者ＩＤが前提となるが、侵入の際には通常は与えられることはない。さらに利用者は、ＩＣカードを紛失した場合には、認証サーバで自分の利用者ＩＤをただちに禁止したり、禁止してもらうことも可能である。

【００３７】ＧＳＭにもとづく防御の別の有利な点は、利用者は、認証処理中はいつでも連絡可能であり、したがって例えばアクセス時に問題があったり、利用者識別に不審がある場合にいつでもシステム担当者から直接呼び出してもらうことができるからである。

【００３８】この方法は安全でコスト的に有利であり、しかも従来からの確かで広範なハードウェアで実現できるという有利な点を有する。

【００３９】また本発明による別の方法は、認証計算機と受信ユニットが1つの装置であることである。

【００４０】

【実施例】本発明による別の有利な点および応用を以下、図を用いて実施例で示す。

【００４１】権限を有する利用者がデータ入力装置（１）を操作する。この装置を介して利用者は、ＴＡＮ（または同等のパスワード）の生成または選択と返信の要求を認証計算機（２）に送信する。認証計算機（２）はＴＡＮ（または同等のパスワード）を生成する。認証計算機（２）には、データ入力装置（１）の利用者の受信器（３）の電話番号またはデータアドレス、例えば電子メールアドレス、網アドレスが既知である。認証計算機（２）は（詳しく図示されていない）受信器（３）にこのＴＡＮ（または同等のパスワード）を送信する。受信器（３）はページャー（３１）または携帯電話（３２）でよい。しかしまた受信器（３）は、（図示されていない）受信箱の電子メールアドレス、テレファックス装置（３３）または音声出力装置であってもよい。音声出力装置は固定的に実装されたスピーカ（３４）または電話（３５）でよい。利用者は、受信器（３）からこのＴＡＮ（または同等のパスワード）を読みとり、または音声出力から聴きとり、データ入力装置（１）に手動で入力する。ここでデータ入力装置（１）は、このＴＡＮ（または同等のパスワード）を認証計算機（２）に送信する。この認証計算機（２）は、このＴＡＮ（または同等のパスワード）がまだ有効であるか否かを検査する。このために認証計算機をプログラムして、ＴＡＮ（または同等のパスワード）の有効性を、ＴＡＮの受信器（３）への送信と、データ入力装置（１）を介してのＴＡＮの伝送との間で時間的に制限するようにしてもよい。この時間的な制限は、例えば2分間としてよい。ＴＡＮ（または同等のパスワード）が有効な場合には、認証計算機（２）は受信ユニット（４）への接続を形成する。利用者はいまやこの接続が継続する間は、データ入力装置（１）から受信ユニット（４）へと送信および／または受信可能な状態にある。

【００４２】このデータをさらに安全にするために暗号化することができることは明らかである。

【００４３】さらに有効性に関して時間的な制限を有するのはＴＡＮ（または同等のパスワード）だけでなく、データ入力装置（１）と受信ユニット（４）との間の接続の継続時間も、時間的に制限することも考えられる。これによりセキュリティホールとなりうる、データ入力装置（１）と受信ユニット（４）との間で形成されるいわゆる「つなぎ放し」を回避することができる。

【００４４】認証計算機（２）と受信ユニット（４）は

9

単一のコンピュータ内に統合化されていてもよい。この場合に、まずデータ処理プログラムへの第1 のアクセスが行われ、このデータ処理プログラムは認証処理（ＴＡＮの生成と伝送）を上記の方法で行う。その後の第2 のステップでデータ伝送が行われる。

【００４５】データ入力装置（１）、認証計算機（２）および受信ユニット（４）までもが1 つのコンピュータであってもよい。この場合に、データ処理プログラムへの第1 のアクセスが行われ、このデータ処理プログラムは認証処理（ＴＡＮの生成と受信器への伝送）を上記の方法で行う。認証後はじめて、利用者は完全な、またはある領域まで制限された計算機へのアクセスを得る。

10

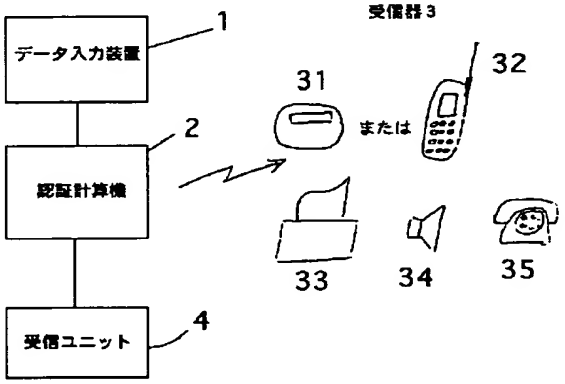
【図面の簡単な説明】

【図1】本発明によるシステムの概略図である。

【符号の説明】

（１）　データ入力装置
（２）　認証計算機
（３）　受信器
（３１）　ページャー
（３２）　携帯電話
（３３）　テレファックス装置
（３４）　スピーカ
（３５）　電話
（４）　受信ユニット

【図1】



フロントページの続き

(51)Int.Cl.[6]		識別記号	FI		
H04Q	7/38		H04M	11/00	303
H04M	11/00	303	H04N	1/44	
H04N	1/44		G09C	1/00	660A
// G09C	1/00	660	H04B	7/26	109S
			H04L	9/00	673A
					673E